AMENDMENTS TO THE CLAIMS

1-32. (Cancelled)

33. (New) A data processor which is supplied with command data specifying a data component to be used for controlling said data processor and operates based on the command data, the command data containing location data of a data component to be used for controlling said data processor, said data processor comprising:

a transmitter/receiver operable to transmit/receive data to/from a server connected over a network;

a validity determination unit operable to determine whether the command data is valid;

a command data processing unit operable to retrieve, when said validity determination unit determines that the command data is valid, the data component specified by the command data, based on the location data contained in the command data; and

a data component processing unit operable to control said data processor based on the data component retrieved by said command data processing unit.

34. (New) The data processor according to claim 33, wherein said data component processing unit is operable to perform a screen display based on the data component retrieved by said command data processing unit.

35. (New) The data processor according to claim 33, wherein said data component processing unit is operable to output the data component retrieved by said command data processing unit to the outside of said data processor.

36. (New) The data processor according to claim 33, wherein the data component used for controlling said data processor by said data component processing unit is limited to be the data component retrieved by said command data processing unit.

37. (New) The data processor according to claim 33, wherein:

the command data is encrypted; and

said validity determination unit is operable to determine whether the command data is valid after decrypting the encrypted command data.

38. (New) The data processor according to claim 33, wherein said command data processing unit includes a language processing section operable to interpret a JAVA language, and a JAVA applet to be processed by said language processing section.

39. (New) The data processor according to claim 38, wherein said transmitter/receiver is operable to receive, in accordance with a user's instruction, the JAVA applet included in said command data processing unit.

40. (New) The data processor according to claim 33, wherein said transmitter/receiver is operable to receive, in accordance with a user's instruction, the command data to be supplied to said validity determination unit.

41. (New) The data processor according to claim 33, wherein said command data processing unit is operable to retrieve the data component from the server by using said transmitter/receiver.

42. (New) The data processor according to claim 33, wherein:

said command data processing unit is operable to determine whether retrieved command data is valid, and

when said command data processing unit determines that the retrieved data component is valid, said data component processing unit is operable to control said data processor based on the data component.

43. (New) A data processing method in which command data specifying a data component to be used for controlling a data processor is supplied, and the command data is used as a basis for an operation, the command data containing location data of a data component to be used for controlling the data processor, said method comprising:

transmitting/receiving data to/from a server connected over a network;

determining whether the command data is valid;

retrieving, when the command data is determined to be valid in said determining whether the command data is valid, the data component specified by the command data, based on the location data contained in the command data; and

controlling the data processor based on the data component retrieved in said retrieving of the data component.

44. (New) The data processing method according to claim 43, wherein said retrieving of the data component retrieves the data component from the server with said transmitting/receiving of the data to/from the server.

45. (New) The data processing method according to claim 43, wherein said retrieving of the command data determines whether the retrieved data component is valid, and, when the data component is determined to be valid in said retrieving of the data component, said controlling of the data processor controls the data processor based on the data component.

46. (New) A data processor for receiving and processing data to which information for tampering detection is added, said data processor comprising:

a receiver operable to receive data which includes an authentication information region for including the tampering detection information, a protected data region for including data to be subjected to tampering detection, and an unprotected data region for including data that is not to be subjected to tampering detection, wherein the protected data region includes an unprotection list which lists, by type, the data included in the unprotected data region;

a protected data authentication unit operable to detect, for the data received by said receiver, whether the data included in the protected data region has been tampered with by using the tampering detection information included in the authentication information region; and

an unprotected data authentication unit operable to authenticate, for the data received by said receiver, whether the data included in the unprotected data region is valid based on the unprotection list which has been confirmed as not having been tampered with by said protected data authentication unit.

47. (New) The data processor according to claim 46, wherein:
the data received by said receiver is hypertext data; and
the unprotection list lists, by type, a tag included in the unprotected data region.

48. (New) A data processor structured by a transmitting data processor and a receiving data processor, said transmitting data processor being operable to transfer, to said receiving data processor, data to which information for tampering detection is added,

wherein said transmitting data processor comprises:

an unprotection list generation unit operable to generate an unprotection list which lists, by type, data that is not to be subjected to tampering detection;

a data generation unit operable to generate data to be transmitted by arranging data to be subjected to tampering detection together with the unprotection list in a protected data region, the data that is not to be subjected to tampering detection in an unprotected data region, and the tampering detection information derived based on the data in the protected data region in an authentication information region; and

a transmitter operable to transmit the data generated by said data generation unit; and

wherein said receiving data processor comprises:

a receiver operable to receive the data transmitted from said transmitting data processor;

a protected data authentication unit operable to detect, for the data received by said receiver, whether the data in the protected data region has been tampered by using the tampering detection information in the authentication information region; and

an unprotected data authentication unit operable to authenticate, for the data received by said receiver, whether the data included in the unprotected data region is valid based on the unprotection list which has been confirmed as not having been tampered with by said protected data authentication unit.

49. (New) The data processor according to claim 48, wherein:
the data generated by said data generation unit is hypertext data; and
the unprotection list lists, by type, a tag included in the unprotected data region.

50. (New) A data processing method for receiving and processing data to which information for tampering detection is added, said method comprising:

receiving data which includes an authentication information region for including the tampering detection information, a protected data region for including data to be subjected to tampering detection, and an unprotected data region for including data that is not to be subjected to tampering detection, the protected data region including an unprotection list which lists, by type, the data included in the unprotected data region;

detecting, for the data received in said receiving of the data, whether the data included in the protected data region has been tampered with by using the tampering detection information included in the authentication information region; and

authenticating, for the data received in said receiving of the data, whether the data included in the unprotected data region is valid based on the unprotection list which has been confirmed as not having been tampered with in said detecting whether the data included in the protected data region has been tampered with.

51. (New) A data processing method for transferring data, to which information for tampering detection is added, from a transmitting data processor to a receiving data processor, wherein:

in the transmitting data processor, said method comprises

generating an unprotection list which lists, by type, data that is not to be subjected to tampering detection,

generating data to be transmitted by arranging data to be subjected to tampering detection together with the unprotection list in a protected data region, the data that is not to be subjected to tampering detection in an unprotected data region, and the tampering detection information derived based on the data in the protected data region in an authentication information region, and

transmitting the data generated in said generating of the data to be transmitted; and

in the receiving data processor, said method comprises

receiving the data transmitted from the transmitting data processor,

detecting, for the data received in said receiving of the data, whether the data in the protected data region has been tampered with by using the tampering detection information in the authentication information region, and

authenticating, for the data received in said receiving of the data, whether the data included in the unprotected data region is valid based on the unprotection list which has been confirmed as not having been tampered with in said detecting whether the data in the protected data region has been tampered with.

52. (New) A data processor for receiving and processing data with a digital signature, said processor comprising:

a receiver operable to receive the data with the digital signature from a server connected over a network;

a signer certificate acquiring unit operable to acquire a signer certificate indicating, by type, what data is signable by a signer of the data received by said receiver; and

a signature authentication unit operable to determine, when the signer certificate acquired by said signer certificate acquiring unit indicates, by type, the data received by said receiver, that a signature applied to the data is valid.

53. (New) The data processor according to claim 52, wherein the signer certificate can include, in a list, by type, a plurality of the signable data.

54. (New) The data processor according to claim 52, wherein:

the signer certificate can include a wildcard as a type of the signable data, and

when the signer certificate acquired by said signer certificate acquiring unit includes the wildcard as the type of the signable data, said signature authentication unit is operable to determine that the signature applied to any data received in said receiver is valid.

55. (New) The data processor according to claim 52, wherein said signature authentication unit is operable to acquire a type of the data based on a characteristic part of a Uniform Resource Identifier of the data received by said receiver.

56. (New) The data processor according to claim 52, wherein said signature authentication unit is operable to acquire the type of the data based on a header part of the data received by said receiver.

57. (New) The data processor according to claim 52, wherein said signer certificate acquiring unit is operable to receive the signer certificate by using said receiver.

58. (New) A data processing method for receiving and processing data with a digital signature, said method comprising:

receiving the data with the digital signature from a server connected over a network;

acquiring a signer certificate indicating, by type, what data is signable by a signer of the data received in said receiving of the data; and

determining, when the signer certificate acquired in said acquiring of the signer certificate indicates, by type, the data received in said receiving of the data, that a signature applied to the data is valid.